I claim:

1. A method of securing communication, where

messages are passed between communicating parties encrypted with a one-time pad, for example by combining bits of a message and bits of the one-time pad using a logical XOR operation, through one channel or a group of channels,

the one-time pad is exchanged between communicating parties through another channel or a group of channels in an encrypted form with the use of private key encryption, for example DES.

2. The method of securing communication of the claim 1, where the one-time pad is generated and passed between communicating parties concurrently with the rest of an application, which uses this secure communication.

3. The method of securing communication of the claim 1, where the one-time pad is entirely generated by one communicating party and used by other communicating parties, and possibly by this one also.

4. The method of securing communication of the claim 1, where the one-time pad consists of two or more parts, each part is generated by a different communicating party and parts are exchanged between communicating parties in an encrypted form.

5. The method of securing communication of the claim 1, where a part of one-time pad is broken into a sequence of pieces and passed between communicating parties in pieces.

6. The method of securing communication of the claim 5, where the additional pieces of one-time pad are generated and passed between communicating parties as needed.